

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for secure loading of secret data from a first ~~security~~ module onboard an administration server to at least one second ~~security~~ module onboard a public payphone terminal, wherein said first module comprises ~~comprising~~ at least one file of secret data associated with at least a type of user card which is used in connection with said second module, said second module comprises a first non-volatile memory and a second volatile memory, ~~characterized in that it comprises the steps of the method comprising:~~
 - [[[-]] generating at least one random data item within the second memory in the second module,
 - [[[-]] recording information comprising said random data item within the first memory of the second module,
 - [[[-]] sending the random data item to the first module,
 - [[[-]] within the first module, encrypting a secret data item in the file of said first module based on the random data item and an encryption algorithm,
 - [[[-]] sending said encrypted secret data item to the second module,
 - [[[-]] transferring information comprising the random data item stored in the first memory of the second module, from said first memory to the second memory of said second module,
 - [[[-]] decrypting said encrypted secret data item, based on a decryption algorithm and the random data item, and recording, within the second module, said decrypted secret data item.
2. (Currently Amended) [[A]] ~~The~~ method according to Claim 1, ~~characterized in that it comprises a further step of further comprising:~~
 - [[[-]] after transferring the information comprising the random data item from the first memory of the second module in the second memory of said module, erasing said information from said first memory.
3. (Cancelled)

4. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~ the steps of generating and sending the random data item as well as recording the information in the second module, are performed by means of a first command.
5. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~ the steps of transferring information decrypting the secret data item in the second module and recording are performed by means of a second command.
6. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~ the information which comprises said random data item, comprises an index relating to a secret data item.
7. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~ several random data items are generated in the second memory of the second module and, after each random data item generation, information comprising the generated random data item is recorded in the first memory of the second module.
8. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~, on each loading operation, a random data item is used for loading a secret data item.
9. (Currently Amended) [[A]] The method according to Claim 1, ~~characterized in that wherein~~, on each loading operation, a unique random data item is used for loading several secret data items.